PATENT ABSTRACTS OF JAPAN

(11)Publication number : **60-102038**
(43)Date of publication of application : **06.06.1985**

(51)Int.Cl. **H04L 9/00**
H04L 13/00

(21)Application number : **58-209173**
(22)Date of filing : **09.11.1983**

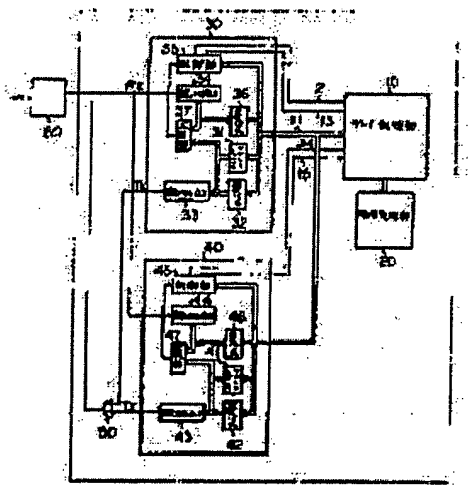
(71)Applicant : **OKI ELECTRIC IND CO LTD**
(72)Inventor : **ARANAKA EIJI**
SAKAMOTO SHUNICHIRO
MIYOSHI HIROYUKI

(54) CIPHER COMMUNICATION SYSTEM

(57)Abstract:

PURPOSE: To improve the transmission efficiency with a simple circuit by setting an address distinguishing cipher data and non-cipher data to an address section of a frame format of a high level data link control means and transmitting and receiving data through the same communication line.

CONSTITUTION: A cipher processing section 20 ciphers data, and a data processing section transfers it to a transmission buffer 32 and requests transmission to control section 35. A communication control LSI30 composes frames of cipher data and transmits the result via a transmission shift register 33, an OR circuit 50, and an MODEM60. The data processing section 10 adds a non-ciphered address to the frame of the non-cipher data via a communication LSI40 and transmits the result via the OR circuit 50 and the MODEM60. In receiving data, it is inputted to reception shift registers 34, 44 from the MODEM, comparator sections 37, 47 detect whether the address of the frame indicates a ciphered message or not, and the ciphered message is subjected to data processing 10 via the LSI30 and the non-ciphered message is subjected to data processing 10 via the LSI40. Thus, mixed messages of the ciphered and the non-ciphered message are transmitted efficiently with a simple circuit.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭60－102038

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和60年(1985)6月6日
H 04 L 9/00		7240－5K	
13/00		C－7240－5K	

審査請求　未請求　発明の数 1　（全5頁）

⑤4発明の名称　暗号通信方式

⑳特　願　昭58－209173

㉒出　願　昭58(1983)11月9日

㉗発明者　新中　栄治　東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内

㉗発明者　坂本　俊一郎　東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内

㉗発明者　三好　裕之　東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内

㉑出願人　沖電気工業株式会社　東京都港区虎ノ門1丁目7番12号

㉔代理人　弁理士　鈴木　敏明

明　細　書

1. 発明の名称

暗号通信方式

2. 特許請求の範囲

ハイレベルデータリンク制御（HDLC）手順のフレームフォーマットを有す暗号データおよび非暗号データが同一の通信路にて伝送される暗号，通信方式において、上記フレームフォーマットのアドレス部を暗号データと非暗号データとでは異なるアドレスとし、該アドレスにより暗号データと非暗号データとを識別して送受信を行うことを特徴とする暗号通信方式。

3. 発明の詳細な説明

（技術分野）

この発明は、データを暗号化して通信する方式に関し、特に暗号データと、非暗号データが同一の通信路にて伝送される暗号通信系に関するものである。

（技術的背景）

データ通信システムが、一般化されてくるにつれ、多量のデータが通信路を流れることになるが、この中には、（例えば、バンキング・システムにおける暗証番号など）部外者に対して機密を必要とするデータもあり、データの暗号化が必要不可欠である。

一方、暗号化処理は、不正な盗聴者による解読が不可能な様に、複雑な変換処理を行っているため、暗号化／復号化には、処理時間がかかり、通信効率が低下する。このため、従来より必要なデータのみ暗号化して暗号データと非暗号データとを同一回線にて通信する方法がとられているが、この場合受信側で受信データが、暗号化されているか否かを知る必要がある。この様な要求を満すために、従来では、以下の様な方式をとっている。

(1) データ通信の前に、次のデータは暗号データか、非暗号データであるか通知する情報を受信側に送信する。

(2) データの一部に、暗号データであるか非暗号データであるかを示す情報を付加する。

(3) データの伝送方式，同期方式をかえて受信

側で識別する。

しかしながら、(1)の方式では、暗号データと非暗号データが頻繁に切替る場合、伝送効率が低下が著しく、(2)の方式では、伝送データの増加をまねき、(3)の方式では、特別な検出器が必要となり汎用の通信制御LSIが単純に使用出来ないという欠点があった。

（発明の目的）

この発明の目的は、上記の問題点を解決し、暗号データと非暗号データを同一の通信路にて通信するための経済的な暗号通信方式を提供することにある。

（発明の概要）

この発明の概要は、ハイレベルデータリンク制御（HDLC）手順のフレームフォーマットのアドレス部を利用して、受信側で暗号データのフレームと非暗号データのフレームを識別することにある。

（実施例）

第1図は、この発明で伝送されるHDLC手順のフレームフォーマットで、1は暗号データのフレーム、2は非暗号データのフレームを表わし、周知の如く、Fはフレーム前後のフラグシーケンス、A1およびA2はアドレス部、E(I)は暗号化されたデータ部、Iは暗号化されていないデータ部、Cは制御部、FCSはフレーム検査シーケンス、をそれぞれ表わしている。受信側では、異なるアドレスA1，A2によって、暗号データ，非暗号データを識別して受信する。

第2図は、この発明の一実施例を示す送受信系のブロック図であり、10は送受信データの処理部、20はデータの暗号化および復号化を行う暗号処理部、30および40はHDLC手順用の通信制御LSIであり、50はQRゲート、60はモデムである。以下図に従って詳細に説明する。

先ず通信を行う前に、暗号処理部20には暗号鍵が、また通信制御LSI 30，40のアドレスレジスタ31，41には、それぞれ暗号データのフレームのアドレスA1、非暗号データのフレームのアドレスA2が設定されており、通信を行う相手装置にも、同様の設定がなされているものとする。

第1に暗号データを送信する場合について説明する。データ処理部10は、暗号処理部20によって、データを暗号化後、通信制御用LSI 30の送信バッファ32にデータバス11を通して送信データを入力し、送信要求線12を用いて、制御部35に送信要求を送出する。しかる後に通信制御用LSI 30は公知の方法によって、第1図の暗号データのフレームを組立てて、送信シフトレジスタ33を介して該フレームをORゲート50へ送出する。よって暗号データは第1図の1に示すフレームフォーマットで、モデム60より送信される。

第2に暗号データを受信する場合について説明する。モデム60によって受信された第1図の1に示す暗号化データのフレームは、通信制御用LSI 30，40の受信シフトレジスタ34，44に入力され、アドレス部の内容がアドレスレジスタ31，41の内容とそれぞれ（比較部37，47で）比較される。今、31には暗号データ通信のためのアドレスA1、41には、非暗号データ通信のためのアドレスA2が設定されているので、通信制御用LSI 30の方だけが、アドレスの一致が検出され、通常の受信動作を行い、受信完了後、制御部35はデータ処理部10に対して、受信通知線13を用い、受信データのあることを通知する。データ処理部10は、暗号データ送受信のための通信制御LSI 30の方から、受信データ在りの通知を受けたことにより、受信データが暗号データであることを認識し、受信バッファ36よりデータバス11を通して受信データを取り込み、暗号処理部20によってこれを復号し、暗号データの受信が終了する。

第3に非暗号化データの送信の場合について説明する。データ処理部10は送信データを非暗号データ送受信のための通信制御LSI 40の送信バッファ42に、データバス11を通して、入力した後送信要求線14を用いて、制御部45に送信要求を送出する。しかる後に通信制御用LSI 40は、公知の方法によって第1図の非暗号データの

フレームを組立てて、送信シフトレジスタ43を介して該フレームをQRゲート50へ送出する。よって非暗号データは、第1図の2に示すフレームフォーマットで、モデム60より送信される。

第4に非暗号データを受信する場合について説明する。モデム60によって受信された第1図の2に示す非暗号データのフレームは、通信制御用LSI30，40の受信シフトレジスタ33，44に入力され、アドレス部の内容がアドレスレジスタ31，41の内容とそれぞれ比較部37，47で比較される。今31には、暗号データ通信のためのアドレスA1、41には、非暗号データ通信のためのアドレスA2が設定されているので、通信制御用LSI40の方だけが、アドレスの一致が検出され、通常の受信動作を行い、受信完了後、制御部45はデータ処理部10に対して、受信通知線15を用い受信データのあることを通知する。データ処理部10は、非暗号データ送受信のための通信制御LSI40の方から、受信データありの通知を受けたことにより、受信データが非暗号データであることを認識し、受信バッファ46よりデータバス11を通して受信データを取り込み、しかるべき処理を行い非暗号データの受信が終了する。

次に、この発明の第2の実施例について説明する。第3図は、この発明の第2の実施例の送受信系ブロック図である。第3図において、第2図と同様の記号は、同等の意味を持つ。以下図に従って詳細に説明する。

先ず通信を行う前に暗号処理部20には暗号鍵が、また通信制御LSI30のアドレスレジスタ31には、暗号データのフレームのアドレスA1が設定されていて、非暗号データのフレームのアドレスA2はグローバルアドレスとして通信を行うものとする。当然のことながら、A1とA2が逆であっても問題はない。ただし第2の実施例は、1対1通信の場合のみ適用され、上記の初期設定は通信を行う相手装置にもなされているものとする。

第1に暗号データおよび非暗号データの送信時について説明する。データ処理部10は、暗号データとして送信する場合は暗号処理部20で暗号化した後、暗号データの送受信のためのアドレスA1をアドレスとして、アドレス部，制御部，暗号化されたデータ部の情報を送信バッファに書き込む。また非暗号データとして送信する場合には、非暗号データの送受信のためのアドレスA2をグローバルアドレスとして、アドレス部制御部，データ部を送信バッファに書き込む。その後通信制御LSI30によって、第1図の1あるいは2のフレームが組立てられて、モデム60より該フレームが送信される。

第2に暗号データおよび非暗号データの受信時について説明する。モデム60に受信された第1図の1あるいは2のフレームは、通信制御LSI30の受信シフトレジスタ34に入力され、アドレス部の内容が比較部37でアドレスレジスタ31の内容と比較されると同時に、グローバルアドレスであるかも検査され、その結果は、制御部35に通知され、アドレスレジスタ31の内容A1との一致あるいはグローバルアドレスA2との一致が検出された場合のみ 制御部35は、ステータスレジスタ38にA1で受信したか、A2で受信したかをフラグとして設定し、通常の受信動作を行い、受信が完了すると、受信通知線13を用いて、データ処理部10に受信データのあることを通知する。データ処理部10は、データバス11を介して、ステータスレジスタ38の内容を検査し、アドレスA1で受信したかアドレスA2すなわちグローバルアドレスで受信したかを識別し、受信データが暗号データか非暗号データかを判断し、暗号データであれば、暗号処理部20で復号して受信が終了する。

（発明の効果）

この発明は、以上説明したようにHDLC手順のフレームフォーマットのアドレス部を利用して、暗号データの送受信時と非暗号データの送受信時とでアドレスを区別することにより、同一通信路にて伝送される両方のデータを受信側で暗号データのフレームと非暗号データのフレームに識別して、

処理を行うようにし、しかも、汎用のLSIを単純に用いただけであるので、従来方式に較べて、特別な検出器等を用いずに制御の単純化を図ることができ、また、本来の伝送情報データ以外に情報を付加することや、暗号データ，非暗号データの区別をする情報をこれらの情報に先行して送信する必要もないので、高い伝送効率を達成できるという利点がある。

4. 図面の簡単な説明

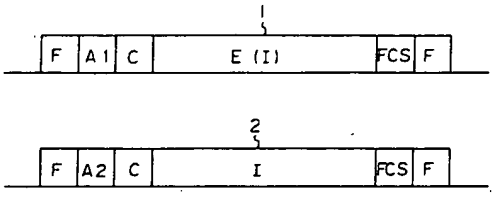
第1図は暗号フレームと非暗号フレームの説明図、第2図は本発明実施例の送受信系ブロック図、第3図は本発明の第2の実施例の送受信系ブロック図である。

1…暗号データのフレーム、2…非暗号データのフレーム、10…データ処理部、20…暗号処理部、30，40…通信制御用LSI、50…QRゲート、60…モデム、11…データバス、12，14…送信要求線、13，15…受信通知線、31，41…アドレスレジスタ、32，42…送信バッファ、33，43…送信シフトレジスタ、34，44…受信シフトレジスタ、35，45…制御部、36，46…受信バッファ、37，47…比較部、38…ステータスレジスタ。

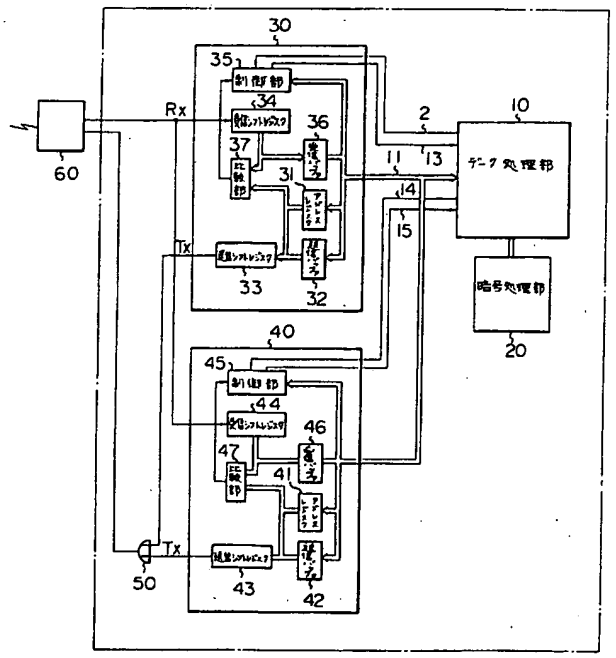
特許出願人　沖電気工業株式会社

代理人　鈴木敏明

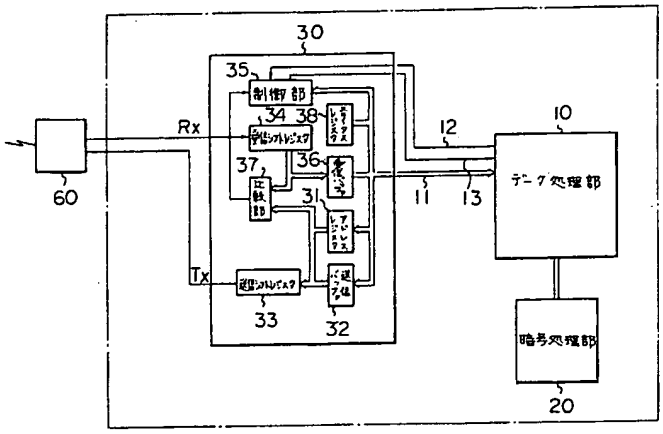
第1図



第2図



第3図



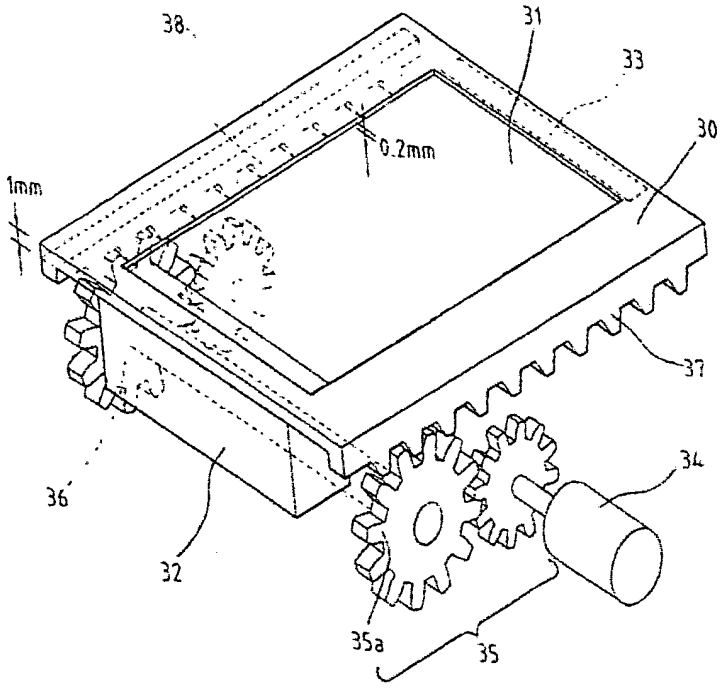


FIG. 3A

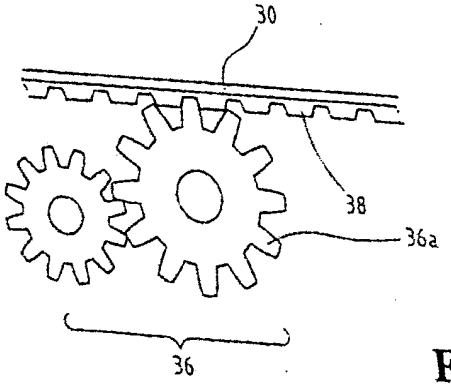


FIG. 3B